**IN THE UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF TEXAS**
**DALLAS DIVISION**

| | |
|---|---|
| BRIAN PATTERSON, *on behalf of himself and all others similarly situated*,<br><br>Plaintiff,<br><br>v.<br><br>AT&T, INC.,<br><br>Defendant. | Case No. 3:24-cv-00875<br><br><br><br><br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Brian Patterson ("Plaintiff") brings this Class Action Complaint against AT&T, Inc. ("Defendant" or "AT&T"), on behalf of himself and all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

## NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII" or "Private Information")[1] including, but not limited to full names, email addresses, mailing addresses, phone numbers, social security numbers, dates of birth, AT&T account numbers and passcodes.[2]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).
[2] https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last visited Apr. 8, 2024).

2. Defendant is an international telecommunications company that provides more than 100 million U.S. consumers with communications experiences across mobile and broadband, with a headquarters in Dallas, Texas.

3. To provide these services, and in the ordinary course of Defendant's business, it acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and Class Members' PII.

4. Plaintiff, on behalf of himself and others similarly situated, seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and the other at least 7.6 million current customers and 65.4 million former account holders who have been impacted[3] by a massive and preventable cyberattack through which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive PII belonging to Plaintiff and Class Members which was being kept unprotected (the "Data Breach").

5. The PII of Plaintiff and Class Members was entrusted to Defendant, its officials, and agents, yet was compromised and unlawfully accessed due to the Data Breach.

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

7. On or about March 30, 2024, AT&T informed many Class Members by email notice and, upon information and belief, mail notice that their sensitive PII had been compromised (the "Notice Letter"). Plaintiff received this letter via email on March 31, 2024 at 10:07 a.m. from

[3] These figures are based on AT&T's "preliminary analysis." *See id.*

sender ATT@message.att-mail.com with the subject line reading "Important update". A copy of the Notice Letter is attached hereto as Exhibit A.

8. AT&T confirmed that Plaintiff's and Class Members' PII have been compromised.[4]

9. Upon information and belief, the Data Breach occurred in 2019 but Defendant did not begin informing victims of the Data Breach until March 30, 2024, approximately five years later. Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until they received Notice Letters from Defendant. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

10. The Notice Letter provides no further information regarding the Data Breach and only recommends that victims reset their passwords, monitor their account activity, and potentially place fraud alert on their account. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiff's and Class Members' PII remains in the possession of criminals.

11. By acquiring, utilizing, and benefiting from Plaintiff's and Class Members' PII for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiff and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiff's and Class Members' PII in its possession and to keep Plaintiff's and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

[4] *Id.*

12. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiff's and Class Members' PII from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiff's and Class Members' PII.

13. Currently, the full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Plaintiff's and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third party.

15. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using

reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

16. Based on the type of sophisticated and targeted criminal activity, the type of PII involved, and Defendant's admission that the PII was accessed, it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiff's and Class Members' PII, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiff's and Class Members' PII – including full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number, and passcode – for the purposes of utilizing or selling the PII for use in future fraud and identity theft activities.

17. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals. The risks associated with the unauthorized disclosure of the PII as to Plaintiff and Class Members will exist for the duration of their respective lifetimes.

18. As Defendant instructed, advised, and warned in its Notice Letter discussed below, Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

19. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the

materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (f) deprivation of value of their PII; (g) invasions of their privacy; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

20. Defendant failed to provide timely, accurate and adequate notice to Plaintiff and Class Members. Plaintiff's and Class Members' knowledge about the PII Defendant allowed to be accessed, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendant's failure to warn impacted persons immediately upon learning of the Data Breach.

21. Plaintiff brings this action on behalf of all persons whose PII was compromised due to Defendant's failure to adequately protect Plaintiff's and Class Members' PII.

## PARTIES

22. Plaintiff Brian Patterson is an adult individual and, at all relevant times herein, a resident and citizen of the state of Pennsylvania, residing in Lawrence County.

23. Defendant AT&T, Inc. is a Texas corporation with its principal place of business at 208 South Akard Street, Dallas, Texas. AT&T's registered agent is CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. Defendant is a citizen of Texas.

## JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of

$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff Patterson, is a citizen of a state different from Defendant.

25. This Court has general personal jurisdiction over Defendant AT&T because Defendant's principal place of business is in the Dallas Division of the Northern District of Texas and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

26. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in the Dallas Division of the Northern District of Texas.

## FACTUAL ALLEGATIONS

***Background***

27. Defendant AT&T is an international telecommunications corporation headquartered in Dallas, Texas. AT&T offers mobile communication services and broadband connectivity to millions of residential and business customers.

28. Defendant's Privacy Policy, posted on its website, states that AT&T "work[s] hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[5]

29. Defendant Privacy Policy also indicates that, "If a breach occurs, we'll notify you as required by law."[6]

[5] *Privacy Policy*, https://about.att.com/privacy/privacy-notice.html (last visited Apr. 8, 2024).
[6] *Id.*

30. The first sentence of Defendant's Notice Letter states, "We take cybersecurity very seriously and privacy is a fundamental commitment at AT&T."[7]

31. Indeed, Defendant has made numerous misleading representations that it would adequately protect Plaintiff's and Class Members' sensitive PII, but has failed to do so.

***Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members***

32. In the ordinary course of its business, AT&T maintains the PII of its customers.

33. Because of the highly sensitive and personal nature of the information Defendant acquires, stores, and has access to, Defendant, upon information and belief, promised to, among other things: keep PII private; comply with industry standards related to data security and PII; inform individuals of their legal duties and comply with all federal and state laws protecting PII; only use and release PII for reasons that relate to business purposes; and provide adequate notice to impacted individuals if their PII is disclosed without authorization.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

35. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

36. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

[7] *See Notice Letter*.

***The Cyberattack and Data Breach***

37. AT&T detected unauthorized access to certain computer systems within its network environment.[8]

38. AT&T took precautionary measures and reset passcodes, as an extra layer of protection for AT&T accounts.[9]

39. Through its investigation, AT&T determined that the data of 7.6 million current AT&T account holders and 65.4 million former account holders were impacted.[10]

40. Upon information and belief, Plaintiff's and Class Members' PII was exfiltrated and stolen in the attack.

41. Furthermore, the investigation determined that the accessed systems contained PII. Upon information and belief, this PII was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

42. The type of PII accessed by the unauthorized actor in the Data Breach includes full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode.[11]

43. While AT&T stated in the Notice Letter that the unusual activity involved data sets from 2019, AT&T did not begin notifying victims until at least March 30, 2024 after AT&T discovered that the PII of Plaintiff and Class Members were posted on the Dark Web.[12]

[8] *See* fn. 2.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

44. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

45. Plaintiff and Class Members provided their PII directly, or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

46. Through its Notice Letter, AT&T also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.

47. Beginning on or around March 30, 2024, Defendant issued Notice Letters by email and mail to Plaintiff and Class Members. In total, at least 73 million individuals were impacted by the Data Breach.[13]

48. The Notice Letters sent to Plaintiff and Class Members stated PII, including full names, email addresses, mailing addresses, phone numbers, social security numbers, dates of birth, AT&T account numbers and passcodes were accessed and exfiltrated in the Data Breach.

49. As a result of the Data Breach, Plaintiff and 73 million Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

50. Defendant waited nearly five years to disclose the Data Brach to Plaintiff and Class Members, and only did so after the PII belonging to Plaintiff and Class Members were posted by

[13] See *id.*

cyber criminals on the Dark Web. As a result of this delay, Plaintiff and Class Members had no idea their PII had been compromised in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

51. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

52. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members.

53. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its consumers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

54. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential static PII, which can be used to commit myriad financial crimes.

55. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use their PII for authorized purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their PII.

56. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential

and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

57. The unencrypted PII of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

58. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII.

***The Data Breach Was Foreseeable***

59. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the finance industry preceding the date of the breach.

60. Considering high profile data breaches at other large companies, Defendant knew or should have known that their electronic records and PII they maintained would be targeted by cybercriminals and ransomware attack groups, and should have been in position to prevent the breach.

61. Indeed, breaches increased 17 percent from 2018 to 2019, and companies in the business sector were targeted more than any other.[14]

[14] *See* "Identity Theft Resource Center®'s Annual End-of-Year Data Breach Report Reveals 17 Percent Increase in Breaches over 2018" https://www.idtheftcenter.org/post/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/ (last visited Apr. 8, 2024).

62. Cyberattacks on telecommunications companies like AT&T have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, potential attack.[15]

***Defendant Had an Obligation to Protect the PII***

63. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

64. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[16] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[17]

65. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

---

[15] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Apr. 8, 2024).

[16] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Apr. 8, 2024).

[17] *Id.*

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third- party service providers have implemented reasonable security measures.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. The FTC enforcement actions include actions against insurance providers and partners like Defendant.

68. Defendant failed to properly implement basic data security practices.

69. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers and other impacted individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. Defendant was at all times fully aware of its obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

***Value of PII***

71. The PII of individuals remains of high value to criminals, as evidenced by the prices criminals will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to

$200, and bank details have a price range of $50 to $200.[18] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

72. Based on the foregoing, the information compromised in the Data Breach, including full names matched with Social Security numbers, is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

73. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[21]

74. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

75. The fraudulent activity resulting from the Data Breach may not come to light for years as there may be a time lag between when harm occurs versus when it is discovered, and also

[18] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Apr. 8, 2024).
[19] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Apr. 8, 2024).
[20] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Apr. 8, 2024).
[21] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 8, 2024).

between when the PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

76. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

77. Plaintiff and Class Members now face a lifetime of constant surveillance of their financial and personal records, credit monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

78. Defendant has acknowledged the risk and harm caused to Plaintiff and Class Members as a result of the Data Breach and encouraged Plaintiff and Class Members to remain vigilant by monitoring account activity and credit reports.

***Defendant Failed to Properly Protect Plaintiff's and Class Members' PII***

79. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Apr. 8, 2024).

80. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

81. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

82. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[23]

83. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for their respective lifetimes.

84. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and

[23] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last visited Apr. 8, 2024).

Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[24]

[24] *Id.* at 3-4.

85. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[25]

[25] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Apr. 8, 2024).

86. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

**Apply principle of least-privilege**

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

**Harden infrastructure**

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[26]

[26] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020). https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Apr. 8, 2024).

87. Moreover, given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

88. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

89. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

90. Because Defendant failed to properly protect and safeguard Plaintiff's and Class Members' PII, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files and exfiltrate that data.

***Defendant Failed to Comply with Industry Standards***

91. As shown above, experts studying cyber security routinely identify insurance providers and partners as being particularly vulnerable to cyberattacks because of the value of the PII which it collects and maintains.

92. Several best practices have been identified that at a minimum should be implemented by insurance providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

93. Other best cybersecurity practices that are standard in the insurance industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such

as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

94. Upon information and belief Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

95. These foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

***Defendant's Negligent Acts and Breaches***

96. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions: failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks; failing to adequately protect PII; failing to properly monitor their own data security systems for existing intrusions; failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures; failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted; failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights; failing to implement policies and procedures to

prevent, detect, contain, and correct security violations; failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports; failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII; failing to train all members of their workforces effectively on the policies and procedures regarding PII; failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals; failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; failing to adhere to industry standards for cybersecurity as discussed above; and, otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

97. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's database, which provided unauthorized actors with unsecured and unencrypted PII.

98. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

## COMMON INJURIES & DAMAGES

99. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

100. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred

mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution or loss of value of their PII; and (i) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

***The Risk of Identity Theft to Plaintiff and Class Members Is Present and Ongoing***

101. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

102. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

103. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

104. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[27] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[28] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

105. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[29] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[30] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[31]

106. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of

[27] Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Apr. 8, 2024).
[28] *Id.*
[29] *What is the Dark Web?* – Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited Apr. 8, 2024).
[30] *Id.*; *see also* Louis DeNicola, *supra* note 25.
[31] *Id.*

an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and do not pay the bills, it damages your credit. You may not find out that someone is using your number until you are turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[32]
>
> What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

107. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[33]

108. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being

[32] Social Security Administration, *Identity Theft and Your Social Security Number* (2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 8, 2024).
[33] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Apr. 8, 2024).

issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[34]

109. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[35]

110. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[36] Defendant did not rapidly report to Plaintiff and Class Members that their PII had been stolen.

111. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

112. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

113. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class

[34] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 8, 2024).
[35] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited Apr. 8, 2024).
[36] *Id.*

Members will need to remain vigilant against unauthorized data use for years or even decades to come.

114. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[37]

115. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[38]

116. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to

[37] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), FTC (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Apr. 8, 2024).

[38] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Apr. 8, 2024).

protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[39]

117. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

***Loss of Time to Mitigate the Risk of Identify Theft and Fraud***

118. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

119. Thus, due to Defendant's admitted recognition of the actual and imminent risk of identity theft, Defendant has encouraged customers to remain vigilant by monitoring account activity and credit reports and to set up free fraud alerts with Equifax, Experian, and TransUnion.

120. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

[39] *See, e.g.*, *Commission Finds LabMD Liable for Unfair Data Security Practices*, FTC, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last visited Apr. 8, 2024).

121. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[40]

122. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[41]

123. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[42]

124. Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to

[40] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 8, 2024).

[41] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Apr. 8, 2024).

[42] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://web.archive.org/web/20190304002224/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Apr. 8, 2024).

remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[43]

***Diminution of Value of the PII***

125. PII is a valuable property right.[44] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

126. PII can sell for as much as $363 per record according to the Infosec Institute.[45]

127. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[46] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[47] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[48]

128. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in

[43] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Apr. 8, 2024).
[44] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[45] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Apr. 8, 2024).
[46] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Apr. 8, 2024).
[47] *See, e.g.* https://datacoup.com/; https://digi.me/.
[48] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Apr. 8, 2024).

its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

***Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary***

129. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

130. Defendant only encourages Plaintiff and Class Members to remain vigilant by monitoring account activity and credit reports and to sign up for free fraud alerts from nationwide credit bureaus — Equifax, Experian, and TransUnion. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to independently sign up for that service.

131. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

132. It must be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

133. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

134. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[49] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

135. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

136. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year, or more, per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

***Injunctive Relief Is Necessary to Protect against Future Data Breaches***

137. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

**Plaintiff's Brian Patterson's Individual Experience**

138. At the time of the Data Breach, Defendant retained Plaintiff Patterson's PII in its system.

[49] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Apr. 8, 2024

139. In order to obtain services from AT&T, Plaintiff Patterson was required to provide his Private Information to AT&T.

140. Plaintiff Patterson received an email notice letter on March 31, 2024, directly from AT&T. According to the Notice Letter, Plaintiff Patterson's account passcode had been compromised, and the information that was improperly accessed and obtained by unauthorized third-parties may have included, Plaintiff's full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode.

141. As a result of the Data Breach, and that the direction of AT&T's Notice Letter, Plaintiff Patterson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, monitoring his financial accounts, and implementing extra security on his computers. Plaintiff Patterson has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Patterson suffered actual injury from having her PII compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of his PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity cost associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in AT&T's possession and is subject to further unauthorized disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect the PII.

142. After the Data Breach, Plaintiff Patterson has come to understand that his PII has been made available on the Dark Web.

143. The Data Breach has caused Plaintiff Patterson to suffer, fear, anxiety, and stress, which has been compounded by the fact that AT&T has still not fully informed him of key details about the Data Breach's occurrence.

144. Plaintiff Patterson anticipates spending considerable time on an ongoing basis to try to mitigate address harms caused by the Data Breach.

145. As a result of the Data Breach, Plaintiff Patterson is at the present risk and will continue to be at increased risk of identity theft and fraud for the rest of his life.

146. Plaintiff Patterson has a continuing interest in ensuring that his PII which, on information and belief, remains backed up in AT&T's possession, is protected and safeguarded from future breaches.

## CLASS ALLEGATIONS

147. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

148. The nationwide class that Plaintiff seeks to represent is defined as follows:

> **All persons identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

149. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

150. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

151. Numerosity: The members of the Class are so numerous that individual joinder of all Class members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of at least 73 million individuals whose sensitive data was compromised in the Data Breach.[50]

152. Commonality: This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: if Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII; if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations; if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards; if Defendant owed a duty to Class Members to safeguard their PII; if Defendant breached their duty to Class Members to safeguard their PII; if Defendant knew or should have known that their data security systems and monitoring processes were deficient; if Defendant should have discovered the Data Breach sooner; if Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct; if Defendant's conduct was negligent; if Defendant's breach implied contracts with Plaintiff and Class Members; if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members; if Defendant failed to provide notice of the Data Breach in a timely manner, and;

[50] See https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last visited Apr. 8, 2024).

if Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

153. Typicality: Plaintiff's claims are typical of the other Class members' claims because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

154. Adequacy: Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including consumer protection litigation. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the interests of the other members of the Class.

155. Superiority: This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision making.

156. Predominance: Common questions of law and fact predominate over any questions affecting only individual Class members. A common pattern and practice of privacy violations are the predominant question to be tried. Individual questions, if any, are relatively minor in relation to the common questions listed above.

157. Ascertainability: Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Defendant's records. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

## CAUSES OF ACTION

### FIRST CAUSE OF ACTION
**NEGLIGENCE**
**(On Behalf of Plaintiff and the Class)**

158. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

159. Plaintiff and the Class entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

160. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

161. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system – and Class Members' PII held within it – to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

162. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

163. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

164. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

165. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

166. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

167. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following: failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII; failing to adequately monitor the security of their networks and systems; failing to have in place mitigation policies and procedures; allowing unauthorized access to Class Members' PII; failing to detect in a timely manner that Class Members'

PII had been compromised; and failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

168. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

169. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

170. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

171. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members' PII.

172. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII – whether by malware or otherwise.

173. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

174. Defendant breached its duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members – which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

175. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

176. Defendant's breach of its common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

## SECOND CAUSE OF ACTION
### INVASION OF PRIVACY
### (On Behalf of Plaintiff and the Class)

177. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

178. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

179. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

180. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

181. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

182. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

183. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

184. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

185. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

186. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with its inadequate cybersecurity system and policies.

187. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

188. Plaintiff, on behalf of himself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

189. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

## THIRD CAUSE OF ACTION
### UNJUST ENRICHMENT
### (On Behalf of Plaintiff and the Class)

190. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

191. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

192. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

193. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

194. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

195. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering insurance related services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

196. Defendant was enriched by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid the data security obligations at the expense of Plaintiff and Class Members by

utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

197. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

198. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

199. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

200. Plaintiff and Class Members have no adequate remedy at law.

201. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to

prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

202. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

203. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

## FOURTH CAUSE OF ACTION
### DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
### (On Behalf of Plaintiff and the Class)

204. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

205. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

206. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

207. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act; Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

208. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its employees' (i.e., Plaintiff and the Class's) data.

209. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

210. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

211. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for

the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2

Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 9, 2024

Respectfully Submitted,

s/ Joe Kendall
JOE KENDALL
Texas Bar No. 11260700
**KENDALL LAW GROUP, PLLC**
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Phone: (214) 744-3000
Fax: (214) 744-3015
jkendall@kendalllawgroup.com

Jeffrey S. Goldenberg (*pro hac vice forthcoming*)
**GOLDENBERG SCHNEIDER, LPA**
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Telephone: (513) 345-8291
jgoldenberg@gs-legal.com

Charles E. Schaffer (*pro hac vice forthcoming*)
**LEVIN SEDRAN & BERMAN**
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500

cschaffer@lfsblaw.com

**LEEDS BROWN LAW, P.C.**
Jeffrey K. Brown (*pro hac vice forthcoming*)
Michael A. Tompkins (*pro hac vice forthcoming*)
Brett R. Cohen (*pro hac vice forthcoming*)
One Old Country Road, Suite 347
Carle Place, NY 11514-1851
Tel: (516) 873-9550
jbrown@leedsbrownlaw.com
mtompkins@leedsbrownlaw.com
bcohen@leedsbrownlaw.com

*Counsel for Plaintiff and the Putative Class*